FORTRA™

ホワイトペーパー (脆弱性管理)

脆弱性管理における5段階の成熟度

クラウドおよびDevOpsの世界で
成熟したVMプログラムを開発し維持する方法

御社の脆弱性管理（VM）プログラムはDevOps、クラウドインフラストラクチャーおよび進化する脅威の環境に対応していますか？多くの組織では、従来のエンタープライズプラットフォームおよびアプリケーションプラットフォーム向けの成熟したVMプログラムがすでに開発されています。しかし、テクノロジーのエコシステムに急激な変化が生じていることは、新しいプラットフォーム上のシステムやプロセスをさまざまな種類の潜在的な脆弱性から保護する必要があることを意味しています。

このホワイトペーパーでは、VMにおける5段階の成熟度について概説します。この文書は、御社の現在の成熟度レベルを知り、DevOpsやクラウドの複雑さがもたらす問題に対処し、御社のセキュリティプログラムを向上させるために必要な取り組みを特定するうえで役立ちます。セキュリティプログラムには昨今のトレンドへの対応が要求されることから、オンデマンドやリアルタイムで実施するアセスメントも、これまで以上に必要とされています。

組織のVMプログラムは、さまざまなレベルの成熟度に分類されます。このホワイトペーパーで紹介する5段階の成熟度は、米国国防総省が開発したプロセス向上のためのモデルである「能力成熟度モデル（CMM）」をベースとしています。

VMプログラムはサイバーセキュリティを成功させるためだけに必要なのではありません。ほとんどの規制ポリシーが、VMプログラムの整備を義務付けています。Center for Internet Security（CIS）は、「クリティカルセキュリティコントロール トップ18」の7番目にVMを挙げています。

能力成熟度モデル

CMMは、段階的かつ定義可能な方法でプロセスを開発および改良するのに役立つモデルです。CMMの5つの段階を以下に説明します。

レベル1：初期

VMプログラムの「初期」のレベルでは、最小限のプロセスと手順が存在します。サードパーティベンダーによるペネトレーションテストまたは外部スキャンの一環として、脆弱性スキャンが実行されます。スキャンは通常1年に1～4回程度、規制要件あるいは監査員の要求に従って行われます。

監査を実施するベンダーが、組織内で発見された脆弱性に関するレポートを提供します。通常組織は「重大なリスク」や「高リスク」の脆弱性を修正して、コンプライアンスの達成または維持を目指します。ひとたびコンプライアンスが達成されたら、一般的に残りの脆弱性情報は放置されます。このレベルの組織は、攻撃者の格好の標的となります。

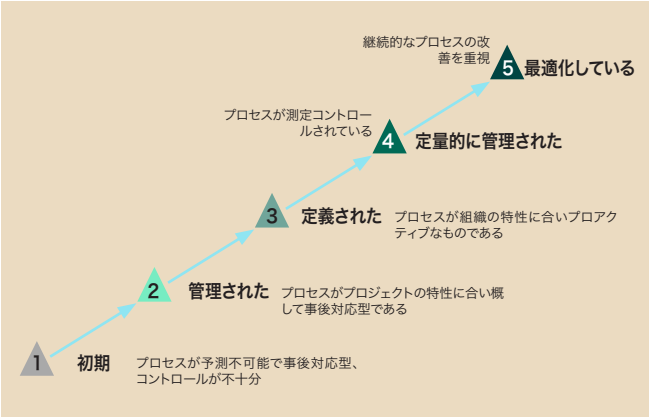
DevOpsチームとクラウドチームが、ITセキュリティプロセスの問題になんとか対応している状態です。コンテナやクラウドイメージの評価を怠っていたり、あるいはサービスプロバイダー環境で利用可能な初歩的なツールのみを使用しています。

レベル2：管理された

VMプログラムにおける「管理された」レベルの組織では、自社内でスキャンを実行します。VMソリューションを入手して、週1回あるいは月1回ベースで定期的なスキャンを行います。対象機器にログインせずにスキャンする「非認証脆弱性スキャン」を実行して、ネットワーク資産の大まかな情報を収集し、セキュリティ管理者が外部者の視点から資産の脆弱性を確認します。

このレベルの組織は、企業上層部の支持を得ておらず、セキュリティに割ける予算が限られています。そのため「安価な」ソリューションを購入することになります。ローエンドのソリューションでも基本的なスキャン機能は提供されますが、データ収集の信頼性、ビジネスコンテキストを取り込む能力、およびオペレーションを自動化し効率を向上させる能力には限界があります。

このレベルの組織のDevOpsおよびクラウドにおいては、クラウド環境内にスキャナーが配置され、ネットワークベースのスキャンやエージェントベースのデータ収集を定期的に実行します。しかしながら、DevOpsワークフローやイメージオーケストレーションとの連携は、ほとんど、あるいはまったくありません。VMプログラムが存在していることを関係者が主張できるように、クラウド環境にセキュリティ機能が採用されてはいるものの、その効果はほとんどないと言えるでしょう。



VMにおける5段階の成熟度

レベル3：定義された

「定義された」レベルの組織では、プロセスと手順が明確に定義されており、組織全体で理解されています。情報セキュリティチームは、経営陣によるサポートとシステム管理者からの信頼を得ています。大多数の組織は、「管理された」レベルから「定義された」レベルの中間付近に属します。

このレベルでは、情報セキュリティチームは、選択したVMソリューションの信頼性が高く、組織のネットワークを安全にスキャンできることを証明できています。認証情報を使用する脆弱性スキャンを毎日または毎週実行し、システム管理者向けには脆弱性レポートを、経営陣用にはリスクトレンドレポートを、というように、利用者に特化したレポートが生成されます。情報セキュリティエコシステム内でVMの状態に関するデータを共有し、これを活用して実用的なインテリジェンスを提供します。重要な資産には、VMエージェントが配置され、認証情報の確認を不要にしつつ、データの収集を合理化しています。

コンテナのデプロイ前には、セキュリティチームとDevOpsチームがオンデマンドでの評価を実施します。クラウドイメージは自動スキャンの対象となります。エージェントベースのデータ収集機能が各イメージに組み込まれ、デプロイ時およびライフサイクルを通してスキャンが行われます。コンテナの評価はチーム間で標準化されており、コンテナが開発パイプラインを通過する前に各コンテナの脆弱性リスクが許容できるレベル内に収まるようにしています。

レベル4：定量的に管理された

VMプログラムが「定量的に管理された」状態にあると、プログラムの特定の属性が定量化され、メトリクスが経営陣に提供されます。このレベルの組織は、クラウド資産とコンテナに対して明確に定義された合否基準を採用しています。また、コンプライアンス違反のイメージやコンテナの修復・破棄に関する方策を定めています。以下は、CISによって推奨されている自動化メトリクスの概要です。

- 組織のVMシステムによるスキャンが最近行われていない組織のビジネスシステムの割合は？
- 組織の各ビジネスシステムの平均的な脆弱性スコアはいくつか？
- 組織の各ビジネスシステムの脆弱性スコアの合計はいくつか？
- OSの更新を1つのビジネスシステムに完全にデプロイするのに平均でどの程度の時間がかかるか？
- アプリケーションソフトウェアの更新を1つのビジネスシステムに完全にデプロイするのに平均でどの程度の時間がかかるか？

これらのメトリクスは、組織全体に対して使用することも、事業部門ごとの分析に使用して、どの部門でリスクを軽減できているか、どの部門の対策が遅れているかなどを判断することもできます。

レベル5：最適化している

最後の「最適化している」レベルの組織では、前の段階で定義されたメトリクスがさらに厳格になります。コンテナの評価は完全自動化され、DevOpsのワークフローに組み込まれます。コンテナに対して許容されるリスクのレベルは、より安全なレベルにまで引き下げられます。脆弱性スキャンおよびコンプライアンススキャンがクラウドオーケストレーションシステムに統合され、ライフサイクルを通して、スケールアップ/ダウン時に自動的に資産をオンボード/オフボードします。情報セキュリティチームと経営陣が協力して達成可能な目標を設定します。それらの目標が着実に達成されれば、継続的なプロセス改善を目指して、新たにより高い目標を設定できます。

DevOpsおよびクラウド環境におけるVM成熟度

成熟した組織でさえ、開発チームがセキュリティチームと対立し、セキュリティを犠牲にしてスピードを優先させようとすることがあります。多くの場合、事業チームやDevOpsチームは、セキュリティチームを避けて、アプリケーションを安全ではない方法でデプロイしています。あなたの組織に優れたVMモデルがすでに導入されているのにもかかわらず、このように進歩が妨げられている場合、どうすれば再びVMプログラムの成熟度を引き上げることができるでしょうか。

Fortraの脆弱性管理ソリューション

最新のクラウドインフラストラクチャーには、認証や動的IPといった制約があるために、エージェントレス型のスキャン機能を使用するセキュリティ担当者はすぐに問題に直面します。エージェントは、クラウドの可視性を高めます。そのため、エラスティック性と拡張性に優れたクラウド環境を採用する企業からの人気が高まっています。エージェントベースの脆弱性管理（ABVM）はFortraのVMソリューションの機能のひとつです。ABVMでは、イメージ内にエージェントをインストールしてデータを収集し、その結果をダッシュボードにレポートの形で表示します。この際に、認証情報や管理サービス用ポートは不要です。また、登録時にスキャンを実行するように設定することもできます。

まとめ

CISコントロールのなかでも、重要なコントロールとされる脆弱性管理は、効果的な情報セキュリティプログラムに実装すべき最重要項目です。脆弱性管理とリスク管理は継続的なプロセスです。そのため、最も効果的なプログラムは、継続的に変化し、組織内のサイバーセキュリティプログラムにおけるリスク低減目標に適応するものでなければなりません。組織の攻撃対象領域を縮小するためには、VMプログラムを継続的に成熟させていくことが不可欠です。

デモのご予約

FortraのVMソリューションのデモを行い、御社のご質問にお答えします。
www.tripwire.com/ja/demoからご予約ください。

出典

1. **www.cisecurity.org/controls/continuous-vulnerability-management/**

FORTRA™

Fortra.com

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。詳細については、fortra.com をご覧ください。